Embassy of the United States of America

American Citizen Services
24 Grosvenor Square
London, W1A 2LQ

PROTECTING YOUR PERSONAL INFORMATION

Often when people belong to online communities, such as email distribution lists, message boards, blogging sites, or social networking sites, they tend to divulge too much personal information about themselves. If you are not careful with the information you reveal on the Internet, it would be very easy for anyone to find your name, phone number, home address, or email address and use this information for social, advertising, or even criminal purposes without your consent. Identity theft can occur when someone steals and uses personal information, such as your name or Social Security number, to commit fraud.

Always be careful and aware of the amount of personal information you share with others, especially online. Before you post any information online, be aware of these general guidelines.

- **Online profiles are public.** When you join an online network or community, you are often required to create a screen name, a password, and to list your e-mail address. You often will be asked to create a user profile with additional information, such as your home address, telephone numbers, birth date, and more. Be aware that in most online communities, members are allowed to view the screen names, email addresses, and sometimes full profiles of other members. Do not post information you are not comfortable sharing with strangers.

- **Comments and information you post on community websites are permanent and not secured.** When you communicate with people online through such media as social networking sites or chat rooms, try not to divulge personal information such as your place of residence, names of family members, or travel dates or plans. All of this information is permanently recorded and can be found by anyone on the Internet. Even if you feel comfortable with the people you are communicating with, do not be lulled into a false sense of security – again, any information you share online can be found by anyone else with Internet access, and may make you vulnerable to spam, scammers, and identity theft.

- **Utilize the privacy settings.** Many social networking sites offer different degrees of privacy settings. These settings allow you to choose and limit the people who can view your profile information and block your name and profile from being available via Internet search engines.

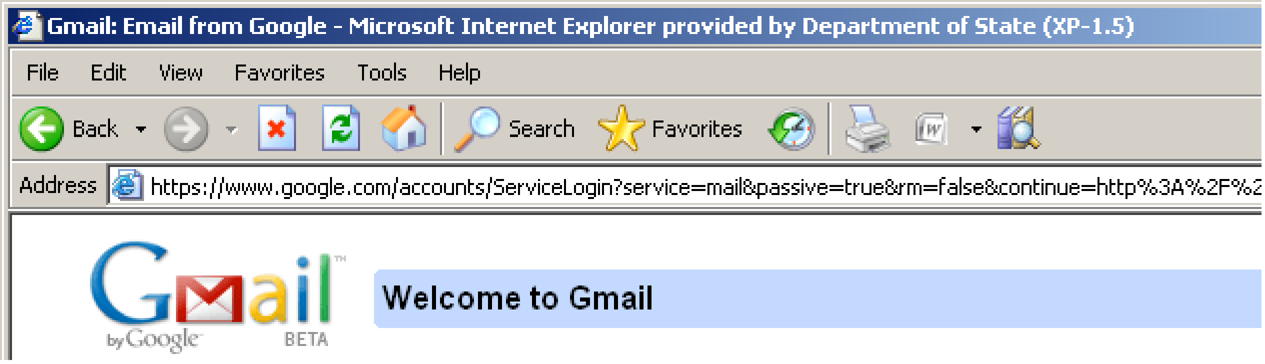
- **Be wary of online surveys**. Chain surveys may seen harmless, but sometimes the questions asked, such as “What was your first pet’s name?” and “What is your mother’s maiden name?" are the same types of security questions asked by banking and credit institutions. Be aware of the information you are making available to the public.

- **Never click on links from your email**. Social networking sites often send you email notifications. Scammers can create email notifications that look just like the real thing. Clicking on such a link can lead to sites that encourage you to enter personal information such as usernames and passwords that allow scammers to hijack your email or social networking accounts, or to download malicious software. In some cases, scammers have used such techniques to obtain money from the user's friends and family by claiming that the user was in a "tragic accident". To protect yourself, never click on the link within an email. Always open your browser and input the web address yourself.

- **Keep an alternative email account**. Only share your primary email account with people you know. By using a secondary email account for your online subscriptions and newsgroups, you can minimize the clutter in your inbox by keeping those emails separate from your personal and business emails. Consider setting up the second email account with non-personal information (e.g. different date of birth, etc.) and write down this information to be placed in a safe location for your own monitoring purposes.

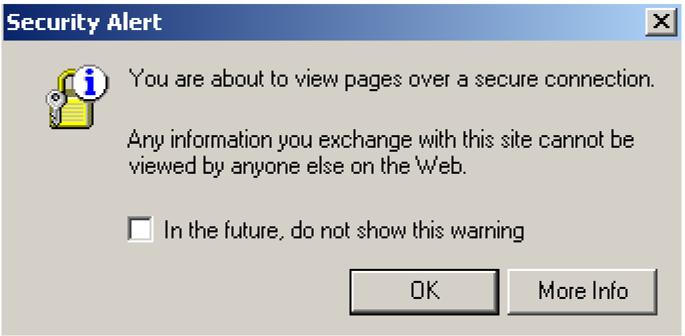
- **When shopping online, buy from reliable sources.** When buying from independent sources (not from established stores or company websites) check the reliability of the seller by reading reviews and buyer feedbacks. When buying expensive items, try to limit your purchases from companies with a clear privacy policy that will explain exactly what information the service will need from you and how that information will be used. Be suspicious if the site does not post a privacy policy.

- **Make sure you enter financial or sensitive information such as usernames and passwords on a secure website.** Make sure that any site that requires you to input credit card or banking information is secure. Look at the URL; if the web address begins with [https://], the website is secure.


Gmail: Email from Google - Microsoft Internet Explorer provided by Department of State (XP-1.5)
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Gmail
by Google
BETA
Welcome to Gmail

Address https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http%3A%2F%2

The default setting for most web browsers is a pop-up window that alerts you whenever you are entering or leaving a secure site.



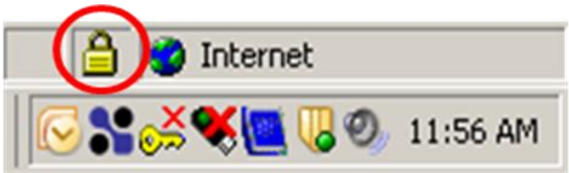
Security Alert

You are about to view pages over a secure connection.

Any information you exchange with this site cannot be viewed by anyone else on the Web.

☐ In the future, do not show this warning

If this option is turned off on your browser, a padlock (indicated inside the red circle in the image below) will appear either on the address bar or in the corner of your browser window to indicate if a site is secure.



- **Do not use the same passwords for all your login sites.** While using the same login name and password is convenient and easy to remember, consider using different passwords or variations of a common password on different sites. This is to ensure the security of your information in case one of your profiles has been hacked. Especially consider using a different password on important websites such as online banking or online payment sites.

- **Consider encrypting the information stored in portable devices.** Many people carry portable devices such as laptops, phones, PDAs, iPods, and USB drives that are capable of carrying significant amounts of information that, when lost, may compromise your personal information. First, be careful of the amount and type of information you carry on portable devices. If you must store highly personal information on these devices, consider encrypting the data. By encrypting your device, the files contained within it become password protected and can normally only be accessed by you or someone who knows your password. Computer programs can be bought to guide you through the encryption process. However, be sure to buy these programs from reputable sources and companies to guarantee the security of your information.